Commonwealth of Massachusetts
Executive Office for Administration and Finance
Information Technology Division

Policy Area: Security	**Policy #:** ITD-SEC-2.00
Title: Enterprise Remote Access Security Policy	

DOCUMENT HISTORY

Date	Proposed By	Summary	Distribution Date

David Lewis

May 8, 2002

David Lewis
Chief Information Officer
Commonwealth of Massachusetts

Effective Date

Table of Contents

INTRODUCTION 3

SCOPE 3

AUTHORIZED AND SUPPORTED REMOTE ACCESS METHODS 3

AGENCY'S REMOTE ACCESS POLICY 5

RELATED POLICIES AND PROCEDURES 6

DEFINITIONS 7

DOCUMENT AUTHORS 9

INTRODUCTION

The Commonwealth of Massachusetts has an information technology (IT) environment to achieve the goals of providing services to its' constituents and support to state's government. This IT environment includes the state Wide Area Network (WAN), also known as the Massachusetts Access to Government Network (MAGNet) made up of more than 170 state agencies, departments, and organizations that maintain local and Enterprise applications (e.g., MMARS, the accounting system). The Information Technology Division (ITD) manages the "Wide Area Network" (WAN) used by Executive Department agencies and other Commonwealth entities. In the past, this network was only available to users who were either physically located in Commonwealth offices or provided with some form of remote access, established as a result of an agency's unilateral deployment/initiatives (e.g., Remote Access Server (RAS), modem bank, etc). The Commonwealth has recently seen an increase, especially as part of its Electronic Government initiative, in the need to extend access to internal systems and information to external customers and business partners. Depending upon their implementation and maintenance, some of these remote access initiatives present an unnecessary level of risk, both to the individual agency and Wide Area Network.

The purpose of this policy is to ensure that remote access to the WAN and all Commonwealth IT domains does not result in an unacceptable level of risk to the security of those systems. Since a security breach committed or caused by one agency WAN user can adversely impact other agency members or the entire environment, all agencies must take responsibility for their system's security by adhering to the requirements of this policy.

Terms used in this policy are defined as set forth in the section entitled "Definitions" on pages 7 and 8. This policy supersedes all previous policies governing remote access to ITD's mainframe and IT environment.

SCOPE

This policy governs the use of remote access by Executive Department[1] agencies. All Executive Department agencies that deploy or otherwise support remote user access are required to comply with this policy. In addition, WAN members and/or users who are not members of the Executive Department, but use remote access must comply with the provisions of this policy as a condition of continued use of, and remote access to, the WAN and other Commonwealth domains.

Agencies must comply with this policy as a prerequisite for access to and/or participation within MAGNet, and/or to use information technology resources managed by ITD. Vendors who seek to develop applications or perform work for the Commonwealth or its' agencies must comply with this and all other Enterprise IT and Security Policies, standards, and guidelines published by ITD. These documents can be accessed at http://www.itd.state.ma.us/spg/publications/standards. Individual agency remote access policies must be developed and maintained by an agency designee.

AUTHORIZED AND SUPPORTED REMOTE ACCESS METHODS

Agencies have deployed a variety of remote WAN access methods, including dial-back remote access servers (RAS), dedicated leased lines, and secure web servers with login authentication, in an effort to meet their business needs. Use of some of these methods has increased

[1] The Executive Department is comprised of the Executive Branch minus the Constitutional Offices, i.e., the State Auditor, State Treasurer, the Attorney General, and the Secretary of the Commonwealth.

administrative overhead and introduced potential security risks for the WAN. In order to minimize risk, use the best and most appropriate remote access technology, and take advantage of economies of scale, agencies must use one of the following authorized remote access services.

Mass.Gov Portal (State's Web Server)
-Query access to agency's databases via portal applications
-Access is provided outside the Commonwealth's WAN (MAGNet)
-Authentication and single sign-on are possible through implementation of the Commonwealth's Security Shared Service (S3)
-SSL encryption is possible
-No access to WAN by a person, only an existing application
-Limited number of authorized protocols
-Requires a DMZ for non-State employee access

Public Access Architecture
-Access is provided through either a central DMZ or extended XDMZ, managed by ITD and located behind the state's perimeter Internet firewalls
-No requirements for additional security infrastructure – agency data classification requirements may drive additional authentication and/or authorization requirements
-SSL encryption is possible
-No access to WAN by a person, only by an existing application

Outlook Web Access (OWA)
-Central service that provides access to electronic mail using the Internet and a Web browser for MassMail users only
-Authentication is provided through user ID and password login

Virtual Private Network (VPN)
-Used to provide employee access to specific internal systems, applications and data
-Access rights are governed by the individual system, application and data
-Authentication and security are always provided through digital certificates and DES encryption for the tunnel; SecuRemote token implementation is also supported
-Tunneling from the WAN to other State and federal sites is supported
-Split tunneling is not allowed
-Additional security infrastructure may be required, including but not limited to data encryption and/or filtering

Unsupported remote access methods will not be authorized after the effective date of this policy without written request that requires authorization for the exception. As of June 30, 2003, agencies must have converted unauthorized or unsupported forms of remote access to enterprise remote access policy supported methods, or have obtained written permission from ITD; through the majority consent of the Enterprise Security Board or its designated subcommittee, to use an alternative form of remote access. Remote access servers with or without dial-back, and IP-to-IP, or "pinhole" methods, will no longer be authorized or supported. Unauthorized methods will be terminated by after June 30, 2003. Only the methods listed above will be in conformance with the Commonwealth's policy.

Agencies that require the use of unsupported methods of remote access (methods not detailed above), such as modem-to-modem connections, or IP-to-IP connections through the firewall, must document and justify their need for the use of such alternative systems. The written justification should specify the particular business needs requiring an alternative implementation and how these alternative remote access mechanisms meet or exceed the performance and security standards provided by the Commonwealth's supported remote access methodologies. The justification must include the number of users who need such alternative access, whether they are employees, contracted business partners, or statutory business partners, and why they cannot use an Enterprise Remote Access policy supported method. The documented proposal should be submitted as quickly as possible to ITD's Enterprise Security Management Unit, via the Customer Coordination Organization at CSB-Support@State.MA.US. The Director of ITD's Enterprise Security Management Unit will submit the document for review by the Enterprise Security Board. The review must occur prior to the implementation, or the continued operation past June 30, 2003, of non-supported remote access methods. The deadline for submission of alternative access requests is December 31, 2002.

The owners (agency heads) of the Commonwealth's IT environments are responsible for the integrity and security of their IT environment. Published findings of violations of security and/or actual loss of control over data may adversely impact the agency's reputation and functioning with today's constituents. External auditors (single auditor or independent auditor), internal auditors, third party auditors and others are taking a greater interest in the integrity of the IT environments of the Commonwealth and its individual agencies. All agencies should be prepared for these auditor reviews. Additionally, ITD will conduct periodic security audits of the Commonwealth's statewide remote access implementation. This will include review and possible modification of any remote access server that does not conform to accepted policy.

AGENCY'S REMOTE ACCESS POLICY

Agencies must adopt and/or maintain a policy that documents that agency's use of authorized and acceptable remote access methodologies. All agencies currently using remote access must either upgrade existing policy or otherwise have such policy in place no later than December 31, 2002. The agency's policy should state that only approved statewide remote access methods will be used for and by employees, contracted business partners, and statutory business partners.

Agency remote access policies must:

1. Describe the types of remote access to be used by the agency as well as the employees, contracted business partners, and statutory business partners who may be authorized for remote access. Agencies should determine the level of access that remote users will have. These levels of access must be differentiated and documented for each user type (i.e., contracted business partners, statutory business partners, telecommuting employees, etc.). Not all methods of remote access are suitable for all types of users. An agency might determine that anyone who is not an employee cannot use a particular remote access method due to security constraints.

2. Identify and mitigate risks associated with transfer of confidential or sensitive data from a secure site to an unsecured device or location (e.g., a notebook or home personal computer). Describe the business needs and related systems, applications, and/or data to which the agency will grant remote access. Authorized remote access users may have the potential, to use the same applications and data that they access at their desktop in the Agency's office. However, an agency should consider specifically disallowing users access to those applications and data that may be inappropriate in an out-of-office environment. For example, accessing personal client information may be inappropriate for home use. The employee, contracted business partner or statutory business partner is responsible for ensuring that their use of the systems does not inappropriately expose the data in the remote environment or compromise security of the systems or applications.

3. Be consistent with the agency's information security data classifications required by the Enterprise Information Security Policy. Agencies must classify their systems, applications and data. Classification will enable the agency to determine the security required for each system and data element. The agency has an obligation, often a statutory requirement, to maintain adequate security over the data. An agency may conclude that some data are too sensitive to access remotely.

4. State that employees, contracted business partners, and statutory business partners are responsible for safeguarding password access provided via an individually assigned Universal Access Identification Code (UAID). Also employees, contracted business partners, and statutory business partners are responsible for safeguarding any other individually assigned passwords necessary for the secure access of Commonwealth information. An employee, contracted business partner, or statutory business partner who has reason to believe that his or her password has been compromised must immediately report this event to the agency's security officer to ensure their password can be reset or their code can be revoked or inactivated. Employees, contracted business partners, and statutory business partners are responsible for all activities performed using their certificates, identification codes, etc.

5. Describe the actions that users must take to ensure the security of remote access sessions. At a minimum, policies must require that remote access users deploy and maintain anti-virus software (using the most up-to-date virus definitions) and personal firewall software on any remote access device.

6. Describe who will be responsible for paying for hardware, software and Internet connections necessary for remote access. Agencies need to determine how they will cover the costs of remote access for different categories of users. Agencies should also determine how much support they will provide to their remote users and how they will pay for that support.

7. Describe the agency's procedures for requesting and/or providing remote access for employees, contracted business partners, and statutory business partners, including the roles of the system administrator and the agency's security officer. These procedures may include, but are not limited to, completion of forms by the employee or business partner to request remote access, approval of the request by the agency's Chief Information Officer or Security Officer, the contractor's project manager, and/or the system administrator, and processing of the forms through the agency's business office. These forms should be kept on file for at least one year after remote access has terminated for each employee, contracted business partner and statutory business partner, and for a longer period of time if so required by the agency's approved records disposition schedule.

8. Require that, prior to obtaining remote access, employees, contracted business partners, and statutory business partners sign an agreement with the agency detailing their responsibilities and obligations regarding use of remote access and the specific files, data, systems and applications which they are authorized to access through remote access. The agreement must contain, at a minimum, the terms of the sample employee, contracted business partner and statutory business partner forms available on the ITD website. The agency must either have its own acceptable use policy or use the Acceptable Use Policy issued by the Executive Office for Administration and Finance. To review Administration and Finance's Acceptable Use Policy, see the http://www.state.ma.us/eoaf/anf-aup.htm website.

9. Describe the agency's remote access security review process. At a minimum, each agency must engage in ongoing remote access security reviews, as well as a comprehensive annual remote access security review to verify the identities of current remote access users and their continuing need for such access. Greater frequency of such reviews may be required based on the sensitivity or confidentiality required by the data being accessed.

RELATED POLICIES AND PROCEDURES

Enterprise policies and procedures for specific remote access methods are either published or under development as follows:

- Mass.Gov Portal – policies under development; current state web site publishing guidelines can be accessed at (http://mass.gov/webmass/)
- Public Access Architecture – current policy can be accessed inside the WAN at ITD's Intranet site (http://www.itd.state.ma.us/spg/projects/OnlineGovernment/SD_2.htm)
- Outlook Web Access (OWA) Procedures
- Security Shared Service Procedures
- VPN Procedures

DEFINITIONS

For purposes of this policy, the following terms are defined:

Acceptable Use Policy is the Administration and Finance Policy on the Use of Information Technology Resources, dated June 16, 1998.

Agency is a department, bureau, commission, board, office, council, or other entity in the executive branch of government, which was created by the constitution or statutes of this State.

Business Partner is a generic term referring to both contracted business partners and statutory business partners.

Contracted Business Partner is an entity under contract with the Commonwealth with which the Commonwealth has an agreement to share data or engage in secure communications for a limited purpose. Contracted business partners do not include individuals who are under contract with and paid directly by the Commonwealth.

DMZ is Demilitarized Zone. DMZ, within the context of this policy is defined as a network added between a protected internal network and an unprotected external network in order to provide a layer of security. A DMZ is sometimes referred to as a "perimeter network". The DMZ is a location where Internet accessible servers are maintained separately from the Internal network. If a DMZ-sited server is breached, it prevents a greater security vulnerability to the internal network.

XDMZ is an eXtended Demilitarized Zone (See DMZ above), in which the DMZ has been deployed either within the internal network, located within the ITD or local agency environment.

Employees are (1) the agency's employees or (2) individuals under contract with the agency to provide services and paid directly by the agency whose work is controlled and directed by the agency.

Hardware includes computers and any physical equipment used in connection with it, such as a keyboards, printers, etc.

Information technology resources are the Commonwealth's computers, printers, and other peripherals, programs, data, local and wide area networks, access to the Internet when provided by the Commonwealth, and remote access methods, including VPN.

MAGNet is the Commonwealth's Wide Area Computer Network.

OWA is Outlook Web Access. OWA is a feature subset of Microsoft Outlook that allows MassMail users to remotely access their email via a web browser.

Owner is the head of the entity. The owner may be commissioner, department head, Chief Justice, Governor, etc., of the agency, department, secretariat, branch of government, authority, or other entity. The owner is ultimately responsible for the information and IT systems within his/her purview. The owner must ensure that the entity for which they are responsible has the security policies and procedures in place to safeguard the information and IT assets of the entity.

Pinhole or IP-to-IP is a rule in a firewall that allows access from a machine outside of a firewall with a specific IP address to machines located inside a firewall with a specific IP address for a specific protocol to be accessed. This method will no longer be supported as of the signed date of this policy. It is anticipated that all pinholes will be eliminated by 6/30/03. As of the date this policy is signed, no new pinholes will be established.

Public Access Architecture Public Access enables the general public and business partners to interface with the state's internal systems via the public network known as the Internet. The Commonwealth's Public Access Architecture is a combination of computers, routers and software that allows public access to occur in a secure manner. Specific policies or rules govern the types of traffic allowed between the Internet and the Public Access Servers and, likewise, between the Public Access Servers and the Internal Network.

Remote Access is all means of access by an individual or entity located outside the Commonwealth's computer systems to those systems.

Software includes programs that run on a computer and process information.

Split Tunneling is a configuration that would allow remote VPN users to access distributed computing resources in both a Local Area Network (LAN) and MAGNet simultaneously. Such concurrent links to a remote LAN and MAGNet can inadvertently cause Commonwealth resources to become susceptible to unpatched, unfiltered, improperly configured, and/or an otherwise vulnerable remote environment.

Statutory Business Partners are individuals or entities that are not under contract with the Commonwealth and have a statutory right to access data held by the Commonwealth.

System Administrator has authority for the overall management and operation of a system or application. The administrator ensures that the operation and/or management of the system or application properly safeguard the data. The application administrator derives their authority from the owner/head of the agency.

UAID is the unique Universal Access Identification Number assigned to each remote access VPN user.

VPN is a Virtual Private Network. A VPN provides an encrypted "tunnel" through which data can flow securely between external users and internal systems.

DOCUMENT AUTHORS

The Enterprise Security Board is composed of thirty-one members, representing the three branches of Massachusetts's government (see below). The Enterprise Security Board developed this policy and recommended it to the Executive Department's Chief Information Officer on April 10, 2002.

General Court of Massachusetts
- Senate
- House of Representatives

Massachusetts Court System
- Supreme Judicial Court
- Trial Court

Executive
- Secretary of State
- Office of the Attorney General
- Office of the State Auditor
- Office of the State Comptroller
- Treasurer and Receiver General
- Massachusetts District Attorneys Association
- Information Technology Division
- Department of Revenue
- Department of Employment and Training
- Executive Office of Health and Human Services
- Human Resources Division
- Operational Services Division
- Massachusetts Teachers' Retirement Board
- Division of Banks
- Executive Office of Public Safety
- Department of Mental Health
- Department of Mental Retardation
- Department of Public Health
- Department of Transitional Assistance
- Massachusetts Highway Department
- Massachusetts Office on Disability
- Department of State Police

Massachusetts Emergency Management Agency
Massachusetts Turnpike Authority
University of Massachusetts, President's Office
Bridgewater State College